대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0053262
Application Number

출 원 년 월 일 : 2003년 07월 31일
Date of Application JUL 31, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 10 월 10 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2003.07.31
【발명의 명칭】	씨씨엠 모드에 따른 암호화 방법 및 이를 수행하기 위한 장치, 씨씨엠 모드에 따른 암호 해독 방법 및 이를 수행하기 위한 장치
【발명의 영문명칭】	METHOD FOR ENCRYPTING IN ACCORDANCE WITH CCM MODE AND APPARATUS FOR PERFORMING THE SAME, METHOD FOR DECRYPTING IN ACCORDANCE WITH CCM MODE AND APPARATUS FOR PERFORMING THE SAME
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	박영우
【대리인코드】	9-1998-000230-2
【포괄위임등록번호】	1999-030203-7
【발명자】	
【성명의 국문표기】	박태건
【성명의 영문표기】	PARK,Tae Gon
【주민등록번호】	700915-1068320
【우편번호】	442-706
【주소】	경기도 수원시 팔달구 망포동 동수원엘지빌리지 108-106
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 박영우 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	21 면 21,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	29 항 1,037,000 원
【합계】	1,087,000 원

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

신속하게 암호화 및 암호 해독 동작을 수행할 수 있는 CCM 모드에 따른 암호화 방법이 개시되어 있다. 상기 암호화 방법은 (a) 1개 이상의 평문 블록들을 순차적으로 제공하는 단계; (b) 제공되는 평문 블록을 CTR 모드를 이용하여 암호화하는 단계; (c) 상기 평문 블록과 제공되는 제 1 블록을 XOR 연산시키는 단계; (d) 상기 XOR 연산에 의해 발생된 블록을 암호화시켜 CBC 암호문 블록을 발생시키는 단계; (e) 상기 CBC 암호문 블록을 이용하여 제 1 블록을 변화시키는 단계; (f) 상기 평문 블록의 다음 평문 블록을 제공하는 단계; (g) 상기 (b) 단계 내지 상기 (f) 단계를 반복시키는 단계; 및 (h) 순차적으로 제공되는 평문 블록들 중 마지막 평문 블록에 상응하여 발생된 CBC 암호문 블록을 상기 CTR 모드를 이용하여 암호화하여 제 2 CTR 암호문 블록을 발생시키는 단계를 포함할 수 있다. 평문 블록들이 메모리로부터 1번 읽혀지기 때문에, 상기 평문 블록들이 신속하게 암호화될 수 있다.

【대표도】

도 1

【색인어】

암호, ENCRYPTION, DECRYPTION, 해독, AES, BLOCK CIPHER

【명세서】

【발명의 명칭】

씨씨엠 모드에 따른 암호화 방법 및 이를 수행하기 위한 장치, 씨씨엠 모드에 따른 암호 해독 방법 및 이를 수행하기 위한 장치{METHOD FOR ENCRYPTING IN ACCORDANCE WITH CCM MODE AND APPARATUS FOR PERFORMING THE SAME, METHOD FOR DECRYPTING IN ACCORDANCE WITH CCM MODE AND APPARATUS FOR PERFORMING THE SAME}

【도면의 간단한 설명】

도 1은 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 따른 암호화 장치의 구성을 도시한 블록도이다.

도 2는 본 발명의 바람직한 일 실시예에 따른 CCM 제어부(암호화 장치에 있어서)의 구성을 도시한 블록도이다.

도 3은 본 발명의 바람직한 일 실시예에 따른 조합부(암호화 장치에 있어서)의 구성을 도시한 블록도이다.

도 4는 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 따른 암호 해독 장치의 구성을 도시한 블록도이다.

도 5는 본 발명의 바람직한 일 실시예에 따른 입력부(암호 해독 장치에 있어서)의 구성을 도시한 블록도이다.

도 6은 본 발명의 바람직한 일 실시예에 따른 CCM 제어부(암호 해독 장치에 있어서)의 구성을 도시한 블록도이다.

도 7은 본 발명의 바람직한 일 실시예에 따른 조합부(암호 해독 장치에 있어서)의 구성을 도시한 블록도이다.

도 8a는 본 발명의 바람직한 일 실시예에 따른 CBC 모드에 의한 동작 과정을 도시한 순서도이다.

도 8b는 본 발명의 바람직한 일 실시예에 따른 CBC 모드를 이용함에 의해 발생된 블록들을 도시한 도면이다.

도 9는 본 발명의 바람직한 일 실시예에 따른 CTR 모드에 의한 암호화 동작을 도시한 순서도이다.

도 10은 본 발명의 바람직한 일 실시예에 따른 CTR 모드에 의한 암호 해독 과정을 도시한 순서도이다.

도 11은 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 의한 1개의 평문 블록에 대한 암호화 동작을 도시한 순서도이다.

도 12는 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 의한 전체적인 암호화 과정을 도시한 순서도이다.

도 13a는 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 의한 암호 해독 과정을 도시한 순서도이다.

도 13b는 본 발명의 바람직한 일 실시예에 따른 암호 해독 과정에 의해 발생된 블록들을 도시한 도면이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<16> 본 발명은 CCM 모드에 따른 암호화 방법 및 이를 수행하기 위한 장치, 암호 해독 방법 및 이를 수행하기 위한 장치에 관한 것으로, 더욱 상세하게는 신속하게 암호화 및 암호 해독 동작을 수행할 수 있는 CCM 모드에 따른 암호화 방법 및 이를 수행하기 위한 장치, 암호 해독 방법 및 이를 수행하기 위한 장치에 관한 것이다.

<17> CCM 모드는 CBC 모드와 CTR 모드의 조합 모드이다. 상기 CTR 모드는 암호화 또는 암호 해독에 사용되며, 상기 CBC 모드는 본문 인증(message authentication)에 사용된다. 상기 CCM 모드를 이용하여 평문 블록을 암호화하는 경우, 제공되는 상기 평문 블록을 상기 CTR 모드를 이용하여 암호화한 후 상기 암호화된 블록을 메모리에 저장하고, 그런 후 상기 평문 블록들을 상기 메모리로부터 다시 읽고, 상기 읽은 평문 블록들을 상기 CBC 모드를 이용하여 암호화하여 본문 인증에 사용하였다. 또한, 종래의 암호 해독 장치는 제공되는 암호문 블록을 상기 CTR 모드를 이용하여 해독한 후 상기 해독된 블록을 상기 메모리에 저장하고, 그런 후 상기 암호문 블록을 상기 메모리로부터 다시 읽고, 상기 읽은 평문 블록들을 상기 CBC 모드를 이용하여 암호화한다. 즉, 종래의 암호화 장치/암호 해독 장치는 상기 평문 블록들/상기 암호문 블록들을 2번 읽기 때문에 암호화/암호 해독 속도가 느리다. 그러므로, 상기 속도를 개선할 수 있는 암호화 장치/암호 해독 장치가 요구된다.

【발명이 이루고자 하는 기술적 과제】

<18> 본 발명은 상기한 바와 같은 종래 기술의 문제점을 해결하기 위한 것으로서, 신속하게 평문 블록들을 암호화할 수 있는 CCM 모드에 따른 암호화 방법 및 이를 수행하기 위한 장치를 제안하는 것을 목적으로 한다.

<19> 본 발명의 다른 목적은, 신속하게 암호문 블록들을 해독할 수 있는 CCM 모드에 따른 암호 해독 방법 및 이를 수행하기 위한 장치를 제안하는 것이다.

【발명의 구성 및 작용】

<20> 상기한 바와 같은 목적을 달성하기 위하여, 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 따른 암호화 방법은 (a) 1개 이상의 평문 블록들을 순차적으로 제공하는 단계; (b) 제공되는 평문 블록을 CTR 모드를 이용하여 암호화하는 단계; (c) 상기 평문 블록과 제공되는 제 1 블록을 XOR 연산시키는 단계; (d) 상기 XOR 연산에 의해 발생된 블록을 암호화시켜 CBC 암호문 블록을 발생시키는 단계; (e) 상기 CBC 암호문 블록을 이용하여 제 1 블록을 변화시키는 단계; (f) 상기 평문 블록의 다음 평문 블록을 제공하는 단계; (g) 상기 (b) 단계 내지 상기 (f) 단계를 반복시키는 단계; 및 (h) 순차적으로 제공되는 평문 블록들 중 마지막 평문 블록에 상응하여 발생된 CBC 암호문 블록을 상기 CTR 모드를 이용하여 암호화하여 제 2 CTR 암호문 블록을 발생시키는 단계를 포함할 수 있다.

<21> 본 발명의 일 실시예에 따른 CCM 모드에 따른 암호 해독 방법은 (a) 1개 이상의 암호문 블록들을 순차적으로 제공하는 단계; (b) 제공되는 암호문 블록을 CTR 모드를 이용하여 해독하는 단계; (c) 상기 해독된 블록인 CTR 해독 블록을 제공하는 단계; (d) 상기 CTR 해독 블록과 제공되는 제 1 블록을 XOR 연산시키는 단계; (e) 상기 XOR 연산에 의해 발생된 블록을 암호화

시켜 CBC 암호문 블록을 발생시키는 단계; (f) 상기 CBC 암호문 블록을 이용하여 상기 제 1 블록을 변화시키는 단계; (g) 상기 암호문 블록의 다음 암호문 블록을 제공하는 단계; 및 (h) 상기 (b) 단계 내지 상기 (g) 단계를 반복시키는 단계를 포함할 수 있다.

<22> 본 발명의 일 실시예에 따른 CCM 모드에 따른 암호화 장치는 제공되는 평문 블록들을 순차적으로 제공하며, 제공되는 마지막 평문 블록에 상응하는 CBC 암호문 블록을 제공하는 입력부; CBC 암호문 블록들에 상응하여 변하는 제 1 블록들 및 상기 평문 블록들에 상응하여 변하는 제 2 블록들을 제공하며, 상기 마지막 평문 블록에 상응하는 CBC 암호문 블록을 제공하는 CCM 제어부; 상기 평문 블록들, 상기 제 1 블록들, 상기 마지막 평문 블록에 상응하는 CBC 암호문 블록 및 암호화된 제 2 블록들을 선택적으로 XOR 연산시키고, 상기 XOR 연산에 의해 생성된 XOR 블록들, 제 1 CTR 암호문 블록들 및 제 2 CTR 암호문 블록을 제공하는 조합부; 및 상기 XOR 블록들을 암호화하여 상기 CBC 암호문 블록들을 생성하고, 상기 제 2 블록들을 암호화하며, 상기 생성된 CBC 암호문 블록들과 상기 암호화된 제 2 블록들을 제공하는 블록 사이퍼를 포함할 수 있다. 또한, CTR 모드에 의해 암호화된 평문 블록들인 상기 제 1 CTR 암호문 블록들 및 상기 제 2 CTR 암호문 블록을 저장하는 출력부를 더 포함할 수 있다.

<23> 본 발명의 일 실시예에 따른 CCM 모드에 따른 암호 해독 장치는 순차적으로 제공되는 암호문 블록들 및 CTR 해독 블록들을 제공하는 입력부; CBC 암호문 블록들에 상응하여 변하는 제 1 블록들 및 상기 암호문 블록들에 상응하여 변하는 제 2 블록들을 제공하는 CCM 제어부; 상기 암호문 블록들과 암호화된 제 2 블록들을 XOR 연산시켜 상기 CTR 해독 블록들을 발생시키고, 상기 CTR 해독 블록들과 상기 제 1 블록들을 XOR 연산시켜 XOR 블록들을 발생시키는 조합부; 상기 XOR 블록들을 암호

화하여 상기 CBC 암호문 블록들을 생성하고, 상기 제 2 블록들을 암호화하며, 상기 생성된 CBC 암호문 블록들과 상기 암호화된 제 2 블록들을 제공하는 블록 사이퍼; 및 CTR 모드에 의해 해독된 암호문 블록인 상기 CTR 해독 블록들을 제공하는 출력부를 포함할 수 있다.

<24> 이하에서는 첨부된 도면을 참조하여 본 발명에 따른 CCM 모드에 따른 암호화 방법 및 이를 수행하기 위한 암호화 장치, CCM 모드에 따른 암호 해독 방법 및 이를 수행하기 위한 암호 해독 장치의 바람직한 실시예를 자세히 설명하도록 한다.

<25> 도 1은 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 따른 암호화 장치의 구성을 도시한 블록도이다.

<26> 도 1을 참조하면, 본 발명의 CCM 모드에 따른 암호화 장치는 입력부(10), CCM 제어부(30), 조합부(50), 블록 사이퍼(70) 및 출력부(90)를 포함할 수 있다.

<27> 상기 CCM 모드는 CBC(cipher block chaining) 모드와 CTR(counter) 모드의 조합 모드이다. 즉, 상기 CCM 모드는 상기 CBC 모드와 CTR 모드 중 하나의 모드로 동작할 수 있을 뿐만 아니라 상기 CBC 모드의 동작과 CTR 모드의 동작을 함께 수행할 수도 있다.

<28> 입력부(10)는 복수의 평문 블록들(plaintexts)을 제공받고, 상기 제공받은 평문 블록들을 저장하며, 상기 평문 블록들을 순차적으로 제공하고, 마지막 평문 블록에 상응하는 CBC 암호문 블록을 제공한다. 상기 마지막 평문 블록에 상응하는 상기 CBC 암호문 블록은 MAC(message authentication code)/MIC(message integrity code)라 불린다. AES(advanced encryption standard) 표준에 있어서, 상기 각 평문

블록들은 길이가 각기 128비트이다. 본 발명의 일 실시예에 따른 CCM 모드에 따른 암호화 장치는 1개의 평문 블록에 대하여 상기 CCM 모드를 이용하여 암호화한 후 다음 평문 블록에 대하여 상기 CCM 모드를 이용하여 암호화하며, 상기의 과정을 순차적으로 제공되는 상기 평문 블록들 전부에 대하여 수행한다. 본 발명의 일 실시예에 따른 입력부(10)는 레지스터이다.

<29> CCM 제어부(30)는 상기 CBC 암호문 블록들을 제공받고, 상기 제공받은 CBC 암호문 블록들을 이용하여 제 1 블록들을 변화시키며, 상기 제 1 블록들, 상기 평문 블록들에 상응하여 변하는 제 2 블록들 및 상기 마지막 평문 블록에 상응하는 상기 CBC 암호문 블록을 제공한다. 본 발명의 일 실시예에 따른 CCM 제어부(30)는 레지스터이다. 그리고, 본 발명의 일 실시예에 따른 상기 제 1 블록은 이니셜 벡터(initial vector)이다.

<30> 조합부(50)는 상기 평문 블록들과 상기 제 1 블록들을 XOR 연산시켜 XOR 블록들을 발생시키고, 상기 평문 블록들과 암호화된 제 2 블록들을 XOR 연산시켜 제 1 CTR 암호문 블록들을 발생시키며, 상기 마지막 평문 블록에 상응하는 CBC 암호문 블록과 상기 마지막 평문 블록에 상응하는 암호화된 제 2 블록을 XOR 연산시켜 제 2 CTR 암호문 블록을 발생시킨다.

<31> 블록 사이퍼(70)는 상기 XOR 블록들을 암호화하여 상기 CBC 암호문 블록들을 생성하고, 상기 제 2 블록들을 암호화시킨다. 상세하게는, 본 발명의 일 실시예에 따른 블록 사이퍼(70)는 상기 XOR 블록들 및 상기 제 2 블록들을 상기 AES 표준을 이용하여 암호화한다.

<32> 출력부(90)는 상기 제 1 CTR 암호문 블록들 및 상기 제 2 CTR 암호문 블록을 저장한다. 본 발명의 일 실시예에 따른 출력부(90)는 레지스터이다.

<33> 본 발명의 CCM 모드에 따른 암호화 장치는 상기 각 평문 블록들을 블록 단위로 순차적으로 암호화시킨다. 상기 암호화 과정은 제어부(미도시)에 의해 제어된다. 그리고, 상기 제어부는 본 발명의 암호화 장치에 포함되어 있을 수도 있고 외부 장치에 포함되어 있을 수도 있다.

<34> 본 발명의 CCM 모드에 따른 암호화 장치는 1개의 평문 블록에 대하여 상기 CBC 모드 및 상기 CTR 모드를 이용하여 암호화한 후 다음 평문 블록을 암호화하므로, 종래의 기술보다 빨리 암호화할 수 있다. 즉, 본 발명의 암호화 장치는 상기 평문 블록들을 메모리로부터 1번 읽기 때문에, 종래의 기술보다 신속하게 상기 평문 블록들을 암호화할 수 있다.

<35> 도 2는 본 발명의 바람직한 일 실시예에 따른 CCM 제어부(암호화 장치에 있어서)의 구성을 도시한 블록도이다.

<36> 도 2를 참조하면, CCM 제어부(30)는 CBC 제어부(100) 및 CTR 제어부(120)를 포함할 수 있다.

<37> CBC 제어부(100)는 제공되는 상기 CBC 암호문 블록들을 이용하여 상기 제 1 블록들을 변화시키고, 상기 제 1 블록들과 상기 마지막 평문 블록에 상응하는 상기 CBC 암호문 블록을 제공한다. 상세하게는, CBC 제어부(100)는 처음 평문 블록에 상응하여 기설정된 제 1 블록을 조합부(50)에 제공하고, 상기 기설정된 제 1 블록에 상응하는 CBC 암호문 블록을 이용하여 상기 기설정된 제 1 블록을 변화시킨다. 상기의 과정이 반복된다.

<38> CTR 제어부(120)는 순차적으로 제공되는 상기 평문 블록들에 상응하여 변하는 상기 제 2 블록들을 블록 사이퍼(70)에 제공한다. 상세하게는, CTR 제어부(120)는 상기 처음 평문 블록에 상응하는 기설정된 제 2 블록을 제공하고, 다음 평문 블록에 상응하는 상기 제 2 블록의 값을 1 증가시킨다. 상기의 과정이 반복된다.

<39> 도 3은 본 발명의 바람직한 일 실시예에 따른 조합부(암호화 장치에 있어서)의 구성을 도시한 블록도이다.

<40> 도 3을 참조하면, 조합부(50)는 제 1 조합부(200) 및 제 2 조합부(220)를 포함할 수 있다.

<41> 제 1 조합부(200)는 상기 평문 블록들과 상기 제 1 블록들을 XOR 연산시켜 상기 XOR 블록들을 발생시킨다. 상세하게는, 제 1 조합부(200)는 상기 처음 평문 블록과 상기 기설정된 제 1 블록을 XOR 연산시키고, 상기 다음 평문 블록과 상기 다음 평문 블록에 상응하는 제 1 블록을 XOR 연산시킨다. 상기의 과정이 반복된다.

<42> 제 2 조합부(220)는 상기 평문 블록들과 상기 암호화된 제 2 블록들을 XOR 연산시켜 상기 제 1 CTR 암호문 블록들을 발생시키고, 상기 마지막 평문 블록에 상응하는 CBC 암호문 블록과 상기 마지막 평문 블록에 상응하는 암호화된 제 2 블록을 XOR 연산시켜 상기 제 2 CTR 암호문 블록을 발생시킨다. 상세하게는, 제 2 조합부(220)는 상기 처음 평문 블록과 상기 처음 평문 블록에 상응하는 암호화된 제 2 블록을 XOR 연산시키고, 상기 다음 평문 블록과 상기 다음 평문 블록에 상응하는 암호화된 제 2 블록을 XOR 연산시킨다. 상기의 과정이 반복된다.

<43> 도 4는 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 따른 암호 해독 장치의 구성을 도시한 블록도이다.

<44> 도 4를 참조하면, 본 발명의 CCM 모드에 따른 암호 해독 장치는 입력부(300), CCM 제어부(320), 조합부(340), 블록 사이퍼(360) 및 출력부(380)를 포함할 수 있다.

<45> 입력부(300)는 암호문(ciphertext) 블록들과 CTR 해독 블록들을 제공받고, 상기 암호문 블록들/보정된 암호문 블록들을 순차적으로 제공하며, 상기 CTR 해독 블록들을 조합부(340)에

제공한다. AES(advanced encryption standard) 표준에 있어서, 상기 각 암호문 블록들은 길이가 각기 128비트이다. 본 발명의 일 실시예에 따른 CCM 모드에 따른 암호 해독 장치는 1개의 암호문 블록을 CCM 모드를 이용하여 해독한 후 다음 암호문 블록을 해독한다. 상기 과정이 반복된다. 상세하게는, CCM 모드에 따른 암호 해독 장치는 각 암호문 블록들에 대하여 상기 CTR 모드를 이용하여 해독한 후 상기 CBC 모드를 이용하여 상기 MAC/MIC를 생성한다.

<46> CCM 제어부(320)는 상기 CBC 암호문 블록들을 제공받고, 상기 제공받은 CBC 암호문 블록들을 이용하여 제 1 블록들을 변화시키며, 상기 제 1 블록들, 상기 암호문 블록들에 상응하여 변하는 제 2 블록들을 제공한다. 본 발명의 일 실시예에 따른 CCM 제어부(320)는 레지스터이다.

<47> 조합부(340)는 상기 암호문 블록들과 암호화된 제 2 블록들을 XOR 연산시켜 상기 CTR 해독 블록들을 발생시키고, 상기 CTR 해독 블록들과 상기 제 1 블록들을 XOR 연산시켜 XOR 블록들을 발생시킨다.

<48> 블록 사이퍼(360)는 상기 XOR 블록들을 암호화하여 상기 CBC 암호문 블록들을 생성하고, 상기 제 2 블록들을 암호화시킨다. 상세하게는, 본 발명의 일 실시예에 따른 블록 사이퍼(70)는 상기 XOR 블록들 및 상기 제 2 블록들을 상기 AES 표준을 이용하여 암호화한다.

<49> 출력부(300)는 제공받은 상기 CTR 해독 블록들을 입력부(300)에 제공한다. 본 발명의 일 실시예에 따른 출력부(300)는 상기 CTR 해독 블록들을 저장하며, 레지스터이다.

<50> 본 발명의 CCM 모드에 따른 암호 해독 장치는 상기 각 암호문 블록들을 블록 단위로 순차적으로 해독시킨다. 상기 암호 해독 과정은 제어부(미도시)에 의해 제어된다. 그리고, 상기

제어부는 본 발명의 암호 해독 장치에 포함되어 있을 수도 있고 외부 장치에 포함되어 있을 수도 있다.

<51> 본 발명의 CCM 모드에 따른 암호 해독 장치는 1개의 암호문 블록을 상기 CCM 모드를 이용하여 해독한 후 다음 암호문 블록을 해독하므로, 종래의 기술보다 신속하게 상기 암호문 블록들을 해독할 수 있다. 즉, 본 발명의 암호 해독 장치는 상기 암호문 블록을 메모리로부터 1번 읽기 때문에, 신속하게 상기 암호문 블록들을 해독할 수 있다.

<52> 도 5는 본 발명의 바람직한 일 실시예에 따른 입력부(암호 해독 장치에 있어서)의 구성을 도시한 블록도이다.

<53> 도 5를 참조하면, 입력부(300)는 입력 레지스터(400) 및 블록 길이 제어부(420)를 포함할 수 있다.

<54> 입력 레지스터(400)는 제공받은 상기 암호문 블록들을 블록 길이 제어부(420)에 순차적으로 제공하고, 제공받은 상기 CTR 해독 블록들을 조합부(340)에 제공한다.

<55> 블록 길이 제어부(420)는 암호문 블록이 평문 블록 시 길이 보정된 블록인 경우, 상기 암호문 블록을 보정한다. 즉, 상기 평문 블록의 길이가 128 비트보다 작은 경우, 상기 평문 블록의 길이를 128 비트로 보정한다. 이 경우, 블록 길이 제어부(420)는 상기 암호문 블록 중 상기 평문 블록 시 보정된 부분을 모두 "0"으로 보정한다.

<56> 도 6은 본 발명의 바람직한 일 실시예에 따른 CCM 제어부(암호 해독 장치에 있어서)의 구성을 도시한 블록도이다.

<57> 도 6을 참조하면, CCM 제어부(320)는 CBC 제어부(500) 및 CTR 제어부(520)를 포함할 수 있다.

<58> CBC 제어부(500)는 제공되는 상기 CBC 암호문 블록들을 이용하여 상기 제 1 블록들을 변화시키고, 상기 제 1 블록들을 제공한다. 상세하게는, CBC 제어부(500)는 처음 평문 블록에 상응하는 기설정된 제 1 블록을 조합부(340)에 제공하고, 상기 기설정된 제 1 블록에 상응하는 CBC 암호문 블록을 이용하여 상기 기설정된 제 1 블록을 변화시킨다. 상기의 과정이 반복된다.

<59> CTR 제어부(520)는 순차적으로 제공되는 상기 암호문 블록들에 상응하여 변하는 상기 제 2 블록들을 블록 사이퍼(360)에 제공한다. 상세하게는, CTR 제어부(520)는 상기 처음 암호문 블록에 상응하는 기설정된 제 2 블록을 제공하고, 다음 암호문 블록에 상응하여 상기 제 2 블록의 값을 1 증가시킨다. 상기의 과정이 반복된다.

<60> 도 7은 본 발명의 바람직한 일 실시예에 따른 조합부(암호 해독 장치에 있어서)의 구성을 도시한 블록도이다.

<61> 도 7을 참조하면, 조합부(340)는 제 1 조합부(600) 및 제 2 조합부(620)를 포함할 수 있다.

<62> 제 1 조합부(600)는 상기 CTR 해독 블록들과 상기 제 1 블록들을 XOR 연산시켜 상기 XOR 블록들을 발생시킨다. 상세하게는, 제 1 조합부(600)는 처음의 암호문 블록에 상응하는 상기 CTR 해독 블록과 상기 기설정된 제 1 블록을 XOR 연산시키고, 상기 다음 CTR 해독 블록과 상기 다음 암호문 블록에 상응하는 제 1 블록을 XOR 연산시킨다. 상기의 과정이 반복된다.

<63> 제 2 조합부(620)는 상기 암호문 블록들과 상기 암호화된 제 2 블록들을 XOR 연산시켜 상기 CTR 해독 블록들을 발생시킨다. 상세하게는, 제 2 조합부(620)는 상기 처음 암호문 블록과 상기 처음 암호문 블록에 상응하는 암호화된 제 2 블록을 XOR 연산시키고, 상기 다음 암호

문 블록과 상기 다음 암호문 블록에 상응하는 암호화된 제 2 블록을 XOR 연산시킨다. 상기의 과정이 반복된다.

<64> 도 8a는 본 발명의 바람직한 일 실시예에 따른 CBC 모드에 의한 동작 과정을 도시한 순서도이다.

<65> 도 8a를 참조하면, 상기 평문 블록들이 제공된다(S100). 이어서, 1개의 평문 블록과 상기 평문 블록에 상응하는 제 1 블록이 XOR 연산되어 XOR 블록을 발생된다(S120). 계속하여, 상기 XOR 블록이 암호화되어 CBC 암호문 블록이 발생된다(S140). 이어서, 상기 평문 블록이 순차적으로 제공되는 상기 평문 블록들 중 마지막 평문 블록인지의 여부가 판단된다(S160). 상기 평문 블록이 상기 마지막 평문 블록이 아닌 경우, 상기 CBC 암호문 블록이 이용됨에 의해 상기 제 1 블록이 변화된다(S180). 반면에, 상기 평문 블록이 상기 마지막 평문 블록인 경우, 동작이 종료된다.

<66> 도 8b는 본 발명의 바람직한 일 실시예에 따른 CBC 모드를 이용함에 의해 발생된 블록들을 도시한 도면이다.

<67> 도 8b에 도시된 바와 같이, 상기 CBC 모드를 이용함에 의해 상기 MAC/MIC가 발생된다.

<68> 도 9는 본 발명의 바람직한 일 실시예에 따른 CTR 모드에 의한 암호화 동작을 도시한 순서도이다.

<69> 도 9를 참조하면, 1개의 평문 블록에 상응하는 제 2 블록이 암호화된다(S300). 이어서, 상기 평문 블록과 상기 암호화된 제 2 블록이 XOR 연산된다(S320). 계속하여, 상기 평문 블록이 상기 마지막 평문 블록인지의 여부가 판단된다(S340). 상기 평문 블록이 상기 마지막 평문

블록이 아닌 경우, 상기 제 2 블록의 값이 1 증가된다(S360). 반면에, 상기 평문 블록이 상기 마지막 평문 블록인 경우, 동작이 종료된다.

<70> 도 10은 본 발명의 바람직한 일 실시예에 따른 CTR 모드에 의한 암호 해독 과정을 도시한 순서도이다.

<71> 도 10을 참조하면, 1개의 암호문 블록이 제공된다(S500). 이어서, 상기 암호문 블록에 상응하는 제 2 블록이 암호화된다(S520). 계속하여, 상기 암호문 블록과 상기 암호화된 제 2 블록이 XOR 연산된다(S540). 이어서, 상기 암호문 블록이 순차적으로 제공되는 상기 암호문 블록들 중 마지막 암호문 블록인지의 여부가 판단된다(S560). 상기 암호문 블록이 상기 마지막 암호문 블록이 아닌 경우, 상기 제 2 블록의 값이 1 증가된다. 반면에, 상기 암호문 블록이 상기 마지막 암호문 블록인 경우, 동작이 종료된다.

<72> 도 11은 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 의한 1개의 평문 블록에 대한 암호화 동작을 도시한 순서도이다.

<73> 도 11을 참조하면, 1개의 평문 블록이 제공된다(S700). 이어서, 상기 평문 블록에 상응하는 제 2 블록이 암호화된다(S720). 계속하여, 상기 평문 블록과 상기 암호화된 제 2 블록이 XOR 연산된다(S740). 이어서, 상기 평문 블록과 상기 평문 블록에 상응하는 제 1 블록이 XOR 연산되어 XOR 블록이 발생된다(S760). 계속하여, 상기 XOR 블록이 암호화된다(S780).

<74> 도 12는 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 의한 전체적인 암호화 과정을 도시한 순서도이다.

<75> 도 12를 참조하면, 제공된 상기 평문 블록들 중 1개의 평문 블록이 제공된다(S800). 이어서, 상기 CTR 모드에 의해 상기 평문 블록이 암호화된다(S820). 계속하여, 상기 CBC 모드에

의해 상기 평문 블록이 암호화된다(S840). 이어서, 상기 평문 블록이 상기 마지막 평문 블록인지의 여부가 판단된다(S860). 상기 평문 블록이 상기 마지막 평문 블록이 아닌 경우, 상기 S800 단계부터 다시 실행된다. 즉, 다음 평문 블록이 제공된다. 반면에, 상기 평문 블록이 상기 마지막 평문 블록인 경우, 상기 마지막 평문 블록에 상응하는 CBC 암호문 블록이 상기 CTR 모드에 의해 암호화된다(S880).

<76> 도 13a는 본 발명의 바람직한 일 실시예에 따른 CCM 모드에 의한 암호 해독 과정을 도시한 순서도이다.

<77> 도 13a를 참조하면, 1개의 암호문 블록이 상기 CTR 모드에 의해 해독되어 상기 암호문 블록에 상응하는 CTR 해독 블록이 발생된다(S1000). 이어서, 상기 CTR 해독 블록이 제공된다(S1020). 계속하여, 상기 암호문 블록이 평문 블록 시 길이 보정된 블록인지의 여부가 판단된다(S1040). 상기 암호문 블록이 길이 보정된 블록인 경우, 상기 CTR 해독 블록 중 상기 보정된 블록에 상응하는 부분이 보정된다(S1060). 반면에, 상기 암호문 블록이 길이 보정된 블록이 아닌 경우, 상기 CTR 해독 블록이 제공된다. 이어서, 상기 CBC 모드에 의해 상기 CTR 해독 블록이 암호화되어 상기 MAC/MIC가 발생된다(S1080). 계속하여, 상기 암호문 블록이 마지막 암호문 블록인지의 여부가 판단된다(S1100). 상기 암호문 블록이 상기 마지막 암호문 블록이 아닌 경우, 상기 S1000 단계부터 다시 실행된다. 반면에, 상기 암호문 블록이 상기 마지막 암호문 블록인 경우, 동작이 종료된다.

<78> 도 13b는 본 발명의 바람직한 일 실시예에 따른 암호 해독 과정에 의해 발생된 블록들을 도시한 도면이다.

<79> 도 13b에 도시된 바와 같이, 상기 암호문 블록들이 상기 CTR 모드에 의해 해

독된 경우, 상기 CTR 해독 블록들이 발생된다. 상기 CTR 해독 블록들은 도 13b에 도시된 바와 같이 복수개의 평문 블록들과 제 1 MAC/제 1 MIC를 가지고 있다. 본 발명의 CCM 모드에 따른 암호 해독 장치는 상기 평문 블록들을 상기 CBC 모드를 이용하여 암호화시켜 제 2 MAC/제 2 MIC를 발생시킨다. 그 결과, 상기 제 2 MAC/MIC가 상기 제 1 MAC/MIC와 같은 경우, 암호화된 상기 평문 블록들이 정확하게 해독된 것이다.

<80> 본 발명의 CCM 모드에 따른 암호/해독 시스템은 암호화 장치 및 암호 해독 장치를 각각 가질 수도 있고, 암호화하고 동시에 암호를 해독할 수 있는 하나의 장치를 가질 수도 있다.

<81> 상기한 본 발명의 바람직한 실시예는 예시의 목적을 위해 개시된 것이고, 본 발명에 대한 통상의 지식을 가지는 당업자라면 본 발명의 사상과 범위 안에서 다양한 수정, 변경, 부가가 가능할 것이며, 이러한 수정, 변경 및 부가는 하기의 특허청구범위에 속하는 것으로 보아야 할 것이다.

【발명의 효과】

<82> 이상에서 설명한 바와 같이, 본 발명의 CCM 모드에 따른 암호화 방법 및 이를 수행하기 위한 장치는 평문 블록들을 메모리로부터 1번 읽기 때문에, 신속하게 상기 평문 블록들을 암호화할 수 있는 장점이 있다.

<83> 아울러, 본 발명의 CCM 모드에 따른 암호 해독 방법 및 이를 수행하기 위한 장치는 암호문 블록들을 메모리로부터 1번 읽기 때문에, 신속하게 상기 암호문 블록들을 해독할 수 있는 장점이 있다.

【특허청구범위】

【청구항 1】

(a) 1개 이상의 평문 블록들을 순차적으로 제공하는 단계;

(b) 제공되는 평문 블록을 씨티알(CTR) 모드를 이용하여 암호화하는 단계;

(c) 상기 평문 블록과 제공되는 제 1 블록을 XOR 연산시키는 단계;

(d) 상기 XOR 연산에 의해 발생된 블록을 암호화시켜 CBC 암호문 블록을 발생시키는 단계;

(e) 상기 CBC 암호문 블록을 이용하여 제 1 블록을 변화시키는 단계;

(f) 상기 평문 블록의 다음 평문 블록을 제공하는 단계;

(g) 상기 (b) 단계 내지 상기 (f) 단계를 반복시키는 단계; 및

(h) 순차적으로 제공되는 평문 블록들 중 마지막 평문 블록에 상응하여 발생된 CBC 암호문 블록을 상기 씨티알(CTR) 모드를 이용하여 암호화하여 제 2 CTR 암호문 블록을 발생시키는 단계를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 방법.

【청구항 2】

제 1 항에 있어서, 상기 (a) 단계는, 상기 제공되는 평문 블록들을 저장하는 단계를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 방법.

【청구항 3】

제 1 항에 있어서, 상기 (b) 단계는,

제공되는 제 2 블록을 암호화하는 단계;

상기 평문 블록과 상기 암호화된 제 2 블록을 XOR 연산시켜 제 1 CTR 암호문 블록을 발생시키는 단계;

상기 제 2 블록의 값을 1 증가시키는 단계; 및

상기 증가된 값을 가지는 제 2 블록을 제공하는 단계를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 방법.

【청구항 4】

제 3 항에 있어서, 상기 (b) 단계는,

상기 제 1 CTR 암호문 블록을 저장하는 단계를 더 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 방법.

【청구항 5】

제 1 항에 있어서, 상기 각 블록들은 길이가 각기 128 비트인 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 방법.

【청구항 6】

(a) 1개 이상의 암호문 블록들을 순차적으로 제공하는 단계;

(b) 제공되는 암호문 블록을 씨티알(CTR) 모드를 이용하여 해독하는 단계;

(c) 상기 해독된 블록인 CTR 해독 블록을 제공하는 단계;

(d) 상기 CTR 해독 블록과 제공되는 제 1 블록을 XOR 연산시키는 단계;

(e) 상기 XOR 연산에 의해 발생된 블록을 암호화시켜 CBC 암호문 블록을 발생시키는 단계;

(f) 상기 CBC 암호문 블록을 이용하여 상기 제 1 블록을 변화시키는 단계;

(g) 상기 암호문 블록의 다음 암호문 블록을 제공하는 단계; 및

(h) 상기 (b) 단계 내지 상기 (g) 단계를 반복시키는 단계를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 방법.

【청구항 7】

제 6 항에 있어서, 상기 (a) 단계는,

상기 암호문 블록들을 저장하는 단계를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 방법.

【청구항 8】

제 6 항에 있어서, 상기 (b) 단계는,

제공되는 제 2 블록을 암호화시키는 단계;

상기 암호문 블록과 상기 암호화된 제 2 블록을 XOR 연산시켜 상기 암호문 블록을 해독하는 단계;

상기 제 2 블록의 값을 1 증가시키는 단계; 및

상기 증가된 값을 가지는 제 2 블록을 제공하는 단계를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 방법.

【청구항 9】

제 6 항에 있어서, 상기 (c) 단계는,

상기 CTR 해독 블록을 저장하는 단계를 더 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 방법.

【청구항 10】

제 6 항에 있어서, 상기 각 블록들은 길이가 각기 128 비트인 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 방법.

【청구항 11】

제 6 항에 있어서, 상기 순차적으로 제공되는 암호문 블록이 평문 블록 시 길이 보정된 블록인지의 여부를 판단하는 단계;

상기 암호문 블록이 길이 보정된 블록인 경우, 상기 암호문 블록에 상응하는 상기 CTR 해독 블록을 보정하는 단계; 및

상기 보정된 CTR 해독 블록을 제공하는 단계를 더 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 방법.

【청구항 12】

제 11 항에 있어서, 상기 보정하는 단계는,

상기 평문 블록 시 보정된 부분에 해당하는 부분의 값들을 모두 0으로 설정하는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 방법.

【청구항 13】

제공되는 평문 블록들을 순차적으로 제공하며, 제공되는 마지막 평문 블록에 상응하는 CBC 암호문 블록을 제공하는 입력부;

CBC 암호문 블록들에 상응하여 변하는 제 1 블록들 및 상기 평문 블록들에 상응하여 변하는 제 2 블록들을 제공하며, 상기 마지막 평문 블록에 상응하는 CBC 암호문 블록을 제공하는 CCM 제어부;

상기 평문 블록들, 상기 제 1 블록들, 상기 마지막 평문 블록에 상응하는 CBC 암호문 블록 및 암호화된 제 2 블록들을 선택적으로 XOR 연산시키고, 상기 XOR 연산에 의해 생성된 XOR 블록들, 제 1 CTR 암호문 블록들 및 제 2 CTR 암호문 블록을 제공하는 조합부; 및

상기 XOR 블록들을 암호화하여 상기 CBC 암호문 블록들을 생성하고, 상기 제 2 블록들을 암호화하며, 상기 생성된 CBC 암호문 블록들과 상기 암호화된 제 2 블록들을 제공하는 블록 사이퍼를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 장치.

【청구항 14】

제 13 항에 있어서, 씨티알(CTR) 모드에 의해 암호화된 평문 블록들인 상기 제 1 CTR 암호문 블록들 및 상기 제 2 CTR 암호문 블록을 저장하는 출력부를 더 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 장치.

【청구항 15】

제 14 항에 있어서, 상기 각 블록들은 길이가 각기 128비트인 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 장치.

【청구항 16】

제 14 항에 있어서, 상기 CCM 제어부는,

상기 CBC 암호문 블록들을 수신하고, 상기 제 1 블록들 및 상기 마지막 평문 블록에 상응하는 CBC 암호문 블록을 제공하는 CBC 제어부; 및

제공되는 상기 평문 블록의 수에 상응하여 값이 변하는 상기 제 2 블록들을 제공하는 CTR 제어부를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 장치.

【청구항 17】

제 16 항에 있어서, 상기 제 2 블록들의 값은 제공되는 상기 평문 블록들의 수에 상응하여 순차적으로 1씩 증가하는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 장치.

【청구항 18】

제 14 항에 있어서, 상기 조합부는,

상기 평문 블록들과 상기 평문 블록들에 상응하는 상기 제 1 블록들을 제 1 XOR 연산시키고, 상기 제 1 XOR 연산에 의해 생성된 상기 XOR 블록들을 제공하는 제 1 조합부; 및

상기 평문 블록들과 상기 암호화된 제 2 블록들을 제 2 XOR 연산시키고, 상기 제 2 XOR 연산에 의해 생성된 상기 제 1 CTR 암호문 블록들을 제공하며, 상기 마지막 평문 블록에 상응하는 CBC 암호문 블록과 상기 마지막 평문 블록에 상응하는 암호화된 제 2 블록을 제 3 XOR 연산시키고, 상기 제 3 XOR 연산에 의해 생성된 상기 제 2 CTR 암호문 블록을 제공하는 제 2 조합부를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 장치.

【청구항 19】

제 18 항에 있어서, 상기 제 1 조합부 및 상기 제 2 조합부는 각기 레지스터인 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 장치.

【청구항 20】

제 14 항에 있어서, 상기 입력부 및 상기 출력부는 각기 레지스터인 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 장치.

【청구항 21】

제 20 항에 있어서, 상기 입력부는 상기 평문 블록들을 저장하는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호화 장치.

【청구항 22】

순차적으로 제공되는 암호문 블록들 및 CTR 해독 블록들을 제공하는 입력부;

CBC 암호문 블록들에 상응하여 변하는 제 1 블록들 및 상기 암호문 블록들에 상응하여 변하는 제 2 블록들을 제공하는 CCM 제어부;

상기 암호문 블록들과 암호화된 제 2 블록들을 XOR 연산시켜 상기 CTR 해독 블록들을 발생시키고, 상기 CTR 해독 블록들과 상기 제 1 블록들을 XOR 연산시켜 XOR 블록들을 발생시키는 조합부;

상기 XOR 블록들을 암호화하여 상기 CBC 암호문 블록들을 생성하고, 상기 제 2 블록들을 암호화하며, 상기 생성된 CBC 암호문 블록들과 상기 암호화된 제 2 블록들을 제공하는 블록 사이퍼; 및

씨티알(CTR) 모드에 의해 해독된 암호문 블록인 상기 CTR 해독 블록들을 제공하는 출력부를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 장치.

【청구항 23】

제 22 항에 있어서, 상기 블록들은 길이가 각기 128 비트인 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 장치.

【청구항 24】

제 22 항에 있어서, 상기 입력부는,

제공되는 상기 암호문 블록들 및 상기 CTR 해독 블록들을 제공하는 입력 레지스터; 및

제공되는 암호문 블록이 평문 블록 시 길이 보정된 블록인 경우, 상기 암호문 블록에 상응하는 상기 CTR 해독 블록을 보정하는 블록 길이 제어부를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 장치.

【청구항 25】

제 22 항에 있어서, 상기 CCM 제어부는,

상기 CBC 암호문 블록들을 이용하여 상기 제 1 블록들을 변화시키는 CBC 제어부; 및

제공되는 상기 암호문 블록들의 수에 상응하여 값이 변하는 상기 제 2 블록들을 제공하는 CTR 제어부를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 장치.

【청구항 26】

제 25 항에 있어서, 상기 CBC 제어부 및 상기 CTR 제어부는 각기 레지스터인 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 장치.

【청구항 27】

제 25 항에 있어서, 상기 제 2 블록의 값은 제공되는 상기 암호문 블록의 수에 상응하여 순차적으로 1씩 증가되는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 장치.

【청구항 28】

제 22 항에 있어서, 상기 조합부는,

상기 CTR 해독 블록들과 상기 제 1 블록들을 XOR 연산시켜 상기 XOR 블록들을 발생시키는 제 1 조합부; 및

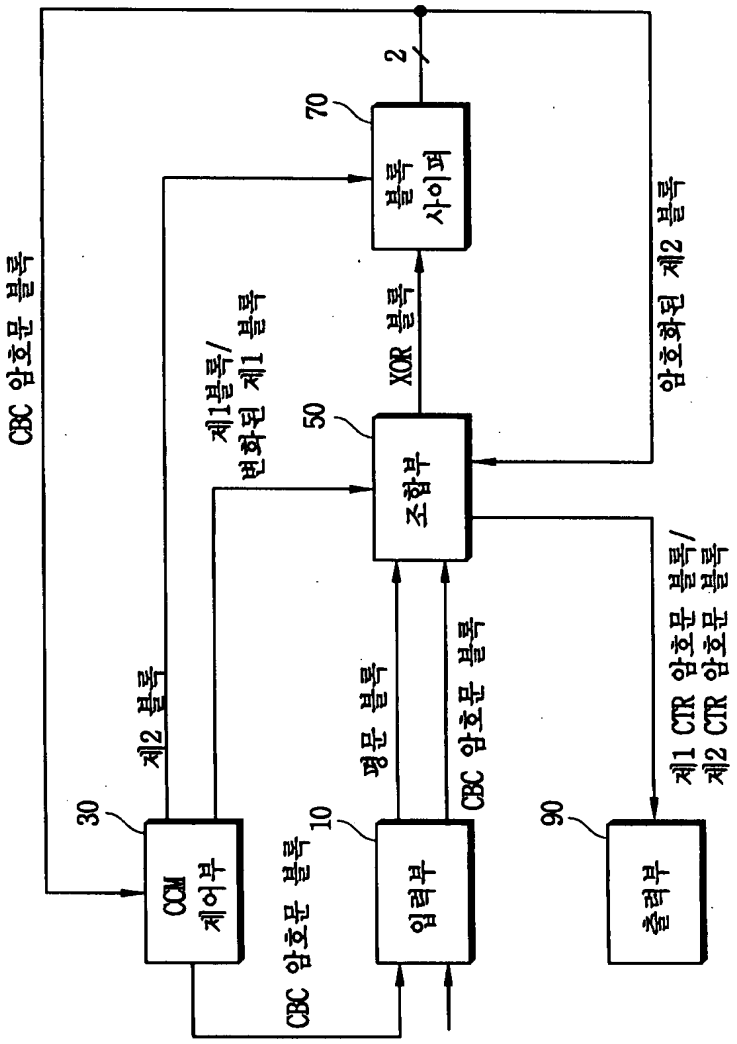
상기 암호문 블록들과 상기 암호화된 제 2 블록들을 XOR 연산시켜 상기 CTR 해독 블록들을 발생시키는 제 2 조합부를 포함하고 있는 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 장치.

【청구항 29】

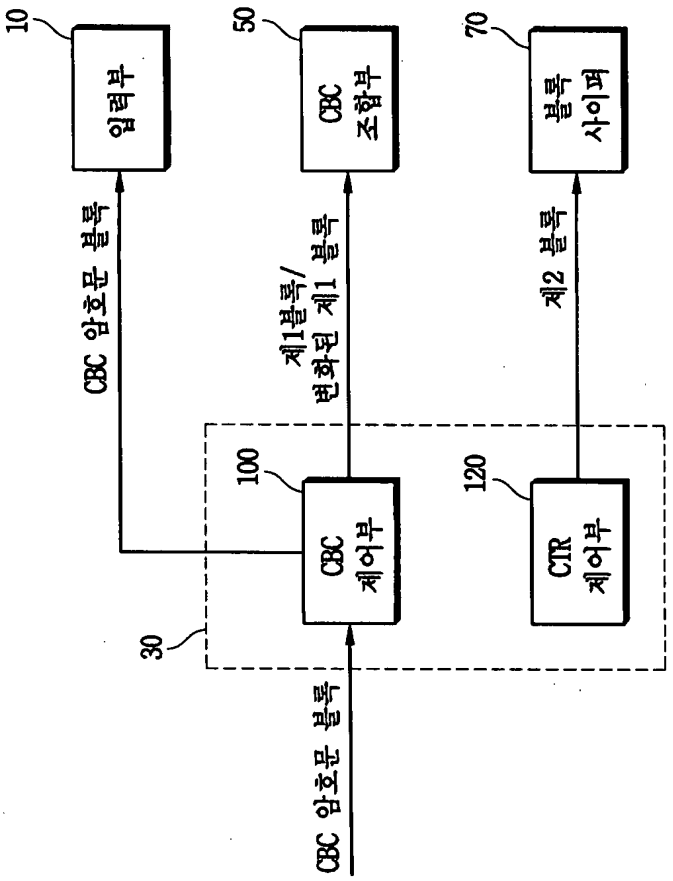
제 22 항에 있어서, 상기 출력부는 레지스터인 것을 특징으로 하는 씨씨엠(CCM) 모드에 따른 암호 해독 장치.

【도면】

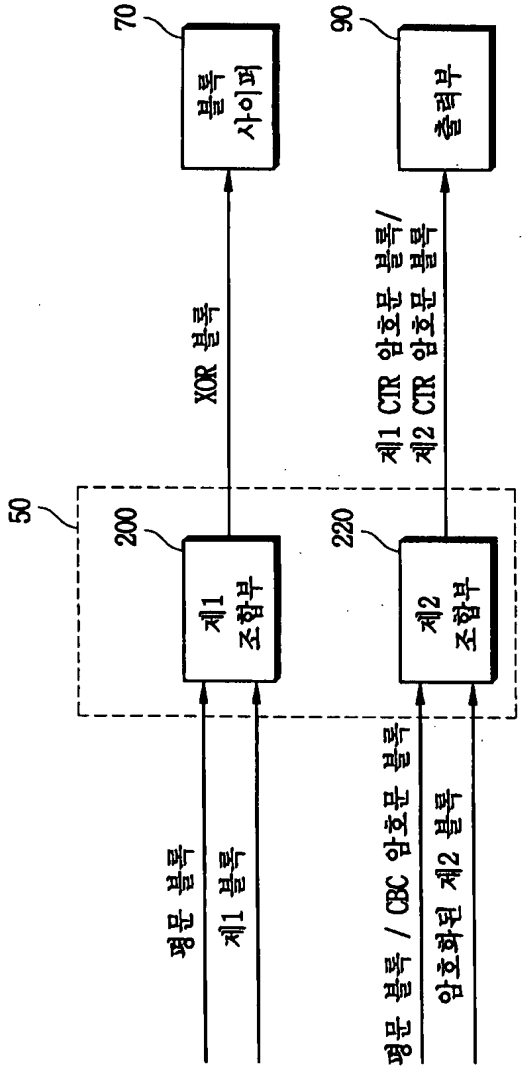
【도 1】


2
70
블록 사이퍼
CBC 암호문 블록
제1블록/ 변화된 제1 블록
XOR 블록
암호화된 제2 블록
50
조합부
제2 블록
평문 블록
CBC 암호문 블록
제1 CTR 암호문 블록/ 제2 CTR 암호문 블록
30
CCM 제어부
10
입력부
90
출력부
CBC 암호문 블록

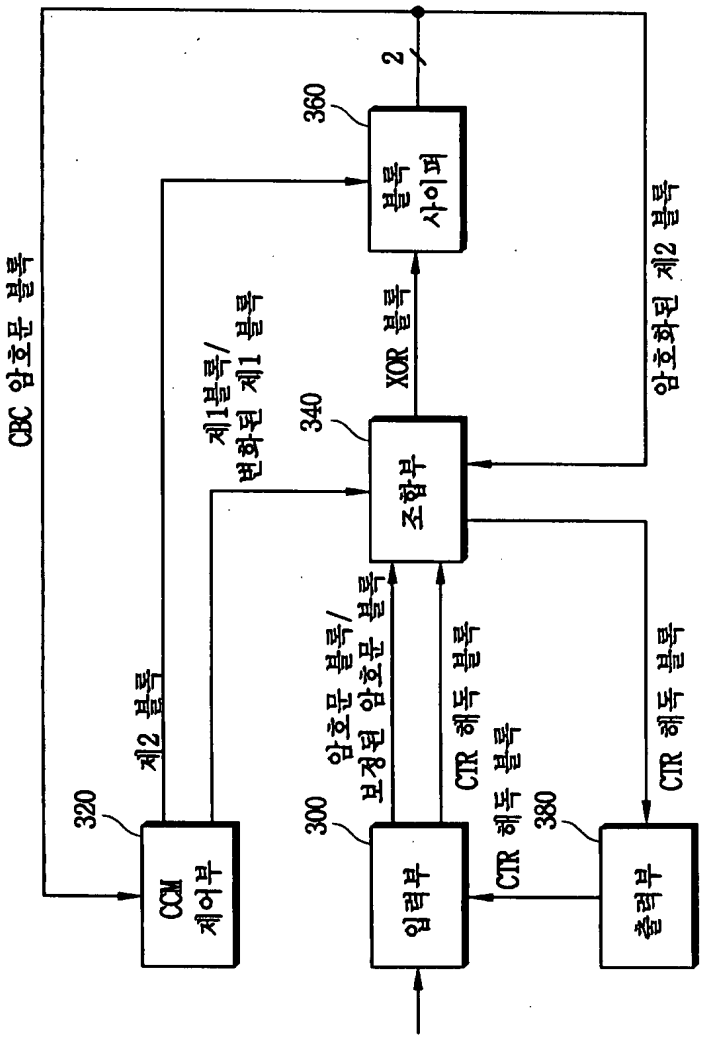
【도 2】


10
입력부
50
CBC 조합부
70
블록 사이퍼
CBC 암호문 블록
제1블록/ 변화된 제1 블록
제2 블록
100
CBC 제어부
120
CTR 제어부
30
CBC 암호문 블록

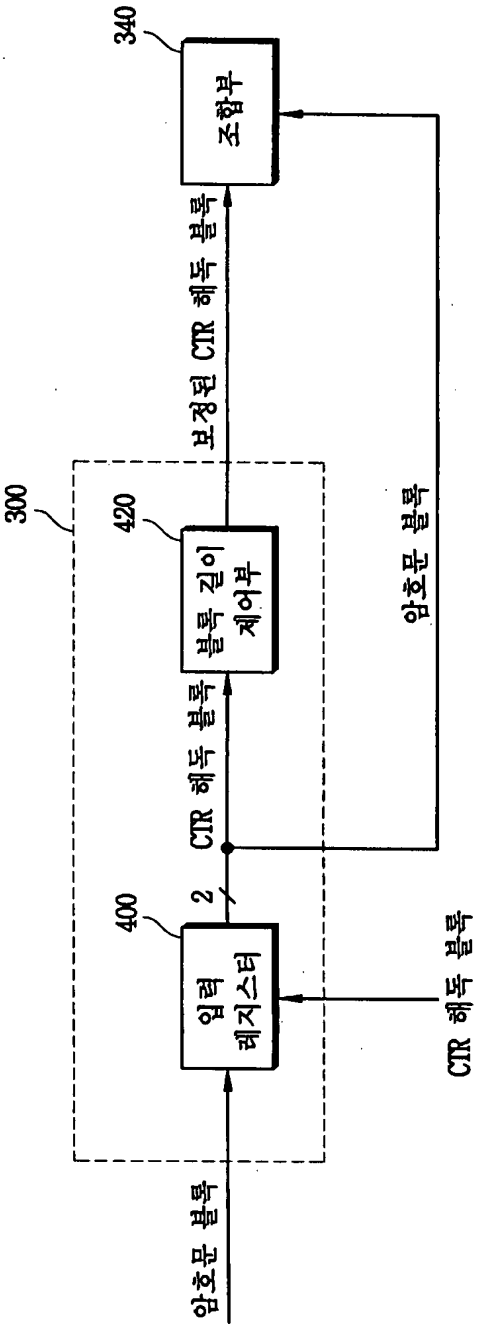
【도 3】


70
블록 사이퍼
90
출력부
XOR 블록
제1 CTR 암호문 블록/
제2 CTR 암호문 블록
50
200
제1 조합부
220
제2 조합부
평문 블록
제1 블록
평문 블록 / CBC 암호문 블록
암호화된 제2 블록

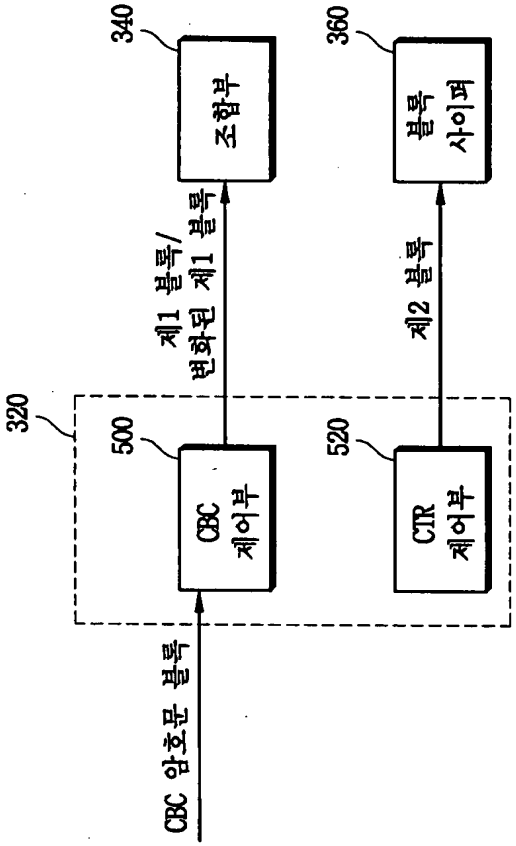
【도 4】


CBC 암호문 블록
제2 블록
320
CCM 제어부
제1블록/ 변화된 제1 블록
340
조합부
XOR 블록
360
블록 사이퍼
2
암호화된 제2 블록
암호문 블록/ 보정된 암호문 블록
300
입력부
CTR 해독 블록
CTR 해독 블록
380
출력부
CTR 해독 블록

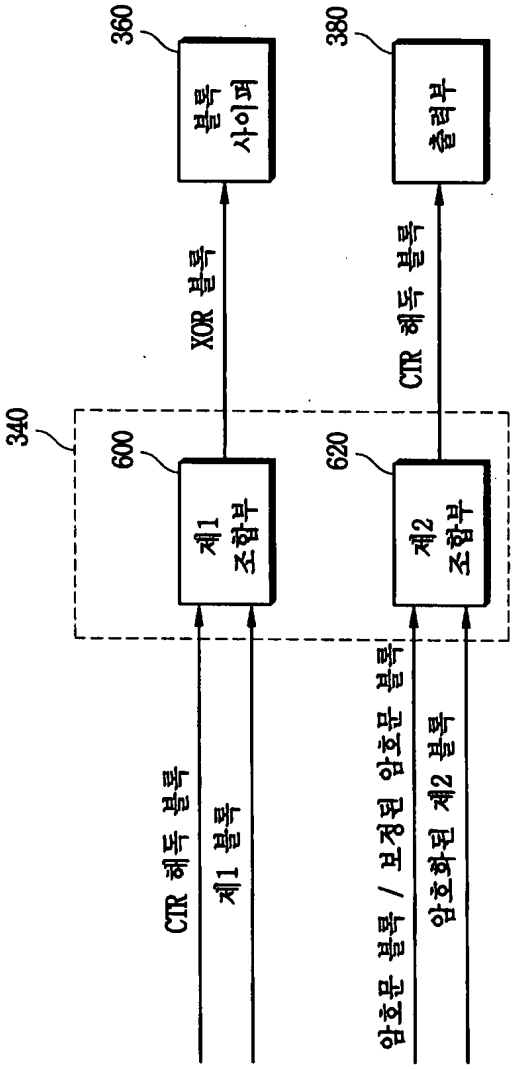
【도 5】


340
조합부
보정된 CTR 해독 블록
300
420
블록 길이 제어부
암호문 블록
CTR 해독 블록
2
400
입력 레지스터
CTR 해독 블록
암호문 블록

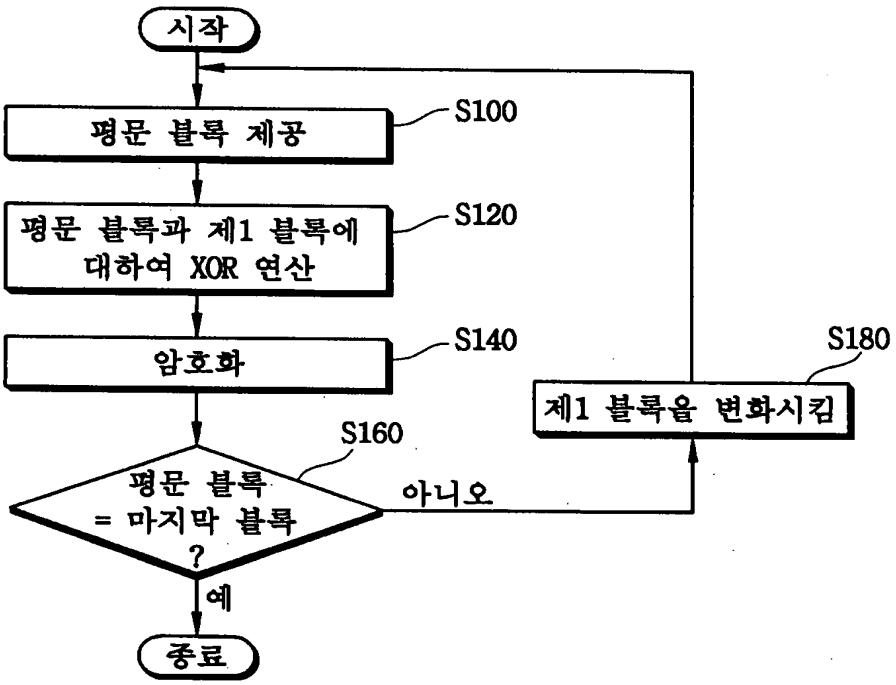
【도 6】


340
조합부
360
블록 사이퍼
제1 블록/
변화된 제1 블록
제2 블록
320
500
CBC 제어부
520
CTR 제어부
CBC 암호문 블록

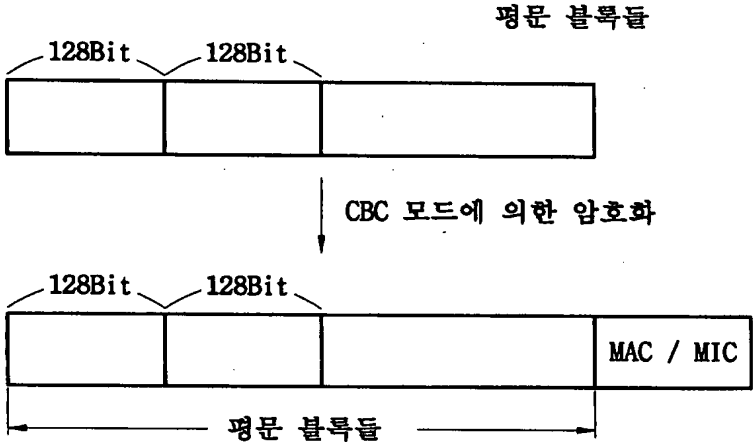
【도 7】


360
블록 사이퍼
380
출력부
XOR 블록
CTR 해독 블록
340
600
제1 조합부
620
제2 조합부
CTR 해독 블록
제1 블록
암호문 블록 / 보정된 암호문 블록
암호화된 제2 블록

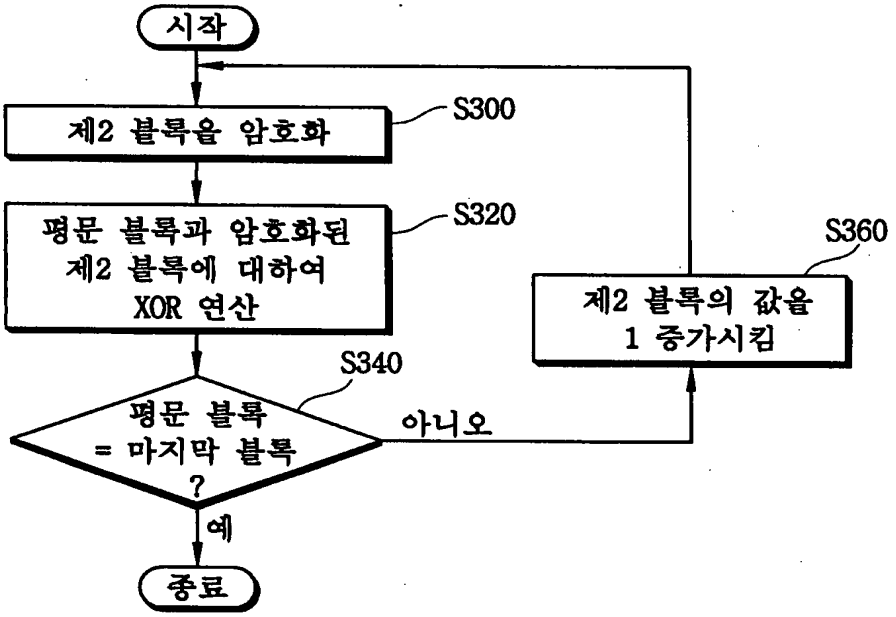
【도 8a】


시작
평문 블록 제공
S100
평문 블록과 제1 블록에 대하여 XOR 연산
S120
암호화
S140
S180
제1 블록을 변화시킴
S160
평문 블록 = 마지막 블록 ?
아니오
예
종료

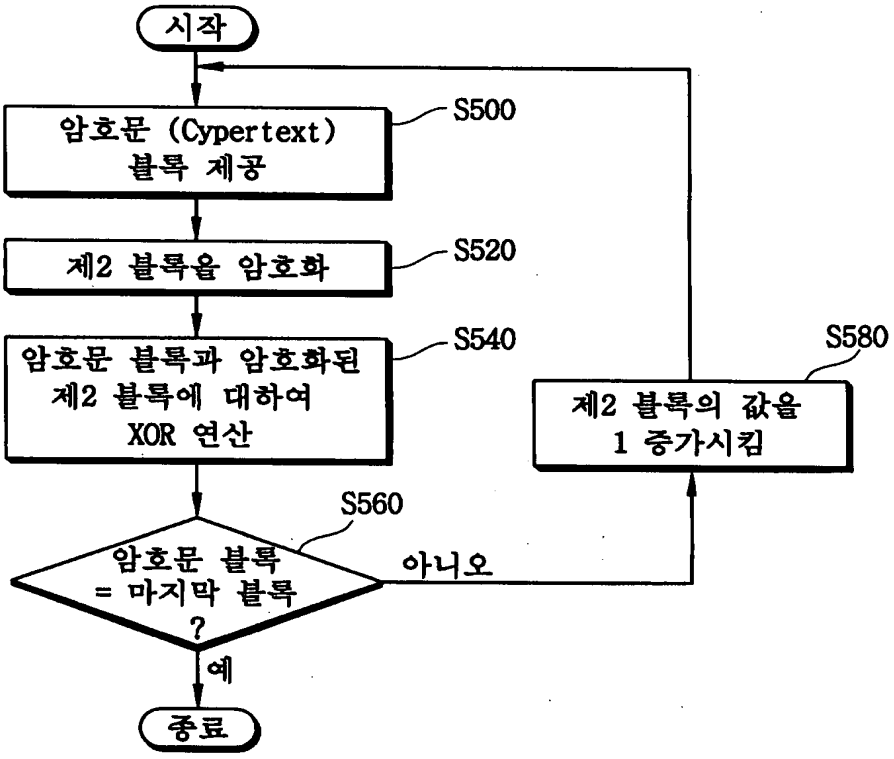
【도 8b】


평문 블록들
128Bit
128Bit
CBC 모드에 의한 암호화
128Bit
128Bit
MAC / MIC
평문 블록들

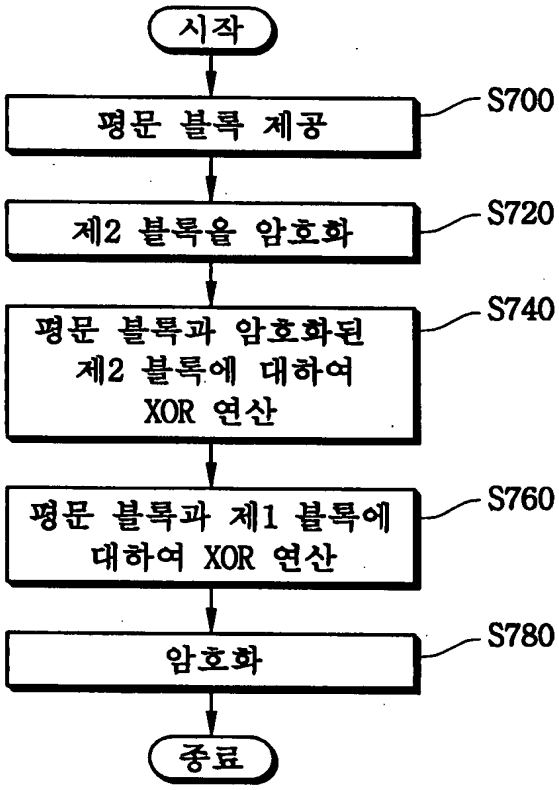
【도 9】


시작
제2 블록을 암호화
S300
평문 블록과 암호화된 제2 블록에 대하여 XOR 연산
S320
S340
평문 블록 = 마지막 블록 ?
아니오
제2 블록의 값을 1 증가시킴
S360
예
종료

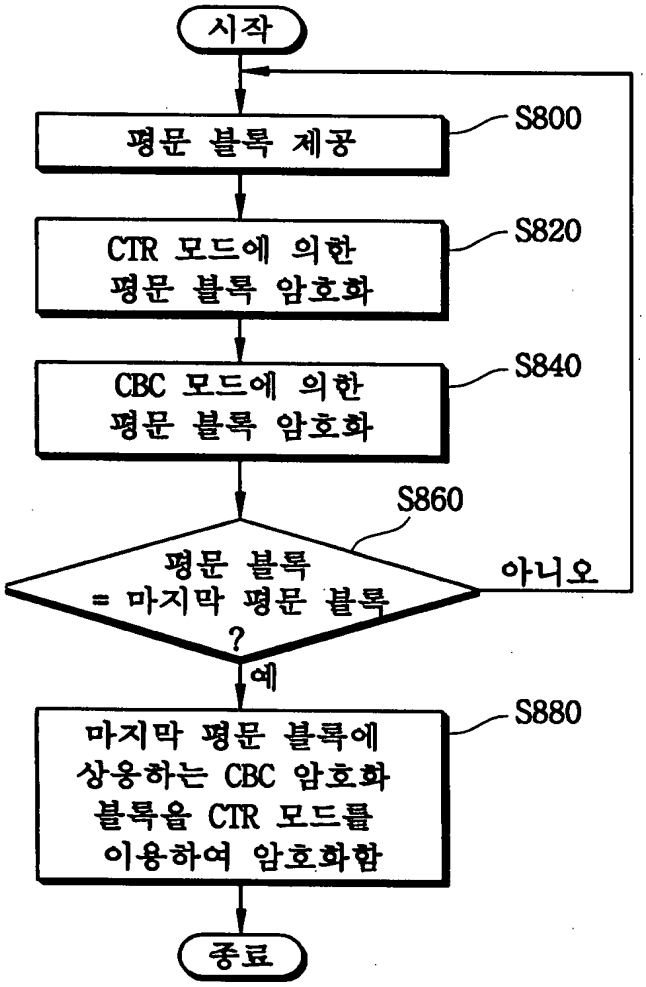
【도 10】


시작
암호문 (Cypertext) 블록 제공
S500
제2 블록을 암호화
S520
암호문 블록과 암호화된 제2 블록에 대하여 XOR 연산
S540
S560
암호문 블록 = 마지막 블록 ?
아니오
제2 블록의 값을 1 증가시킴
S580
예
종료

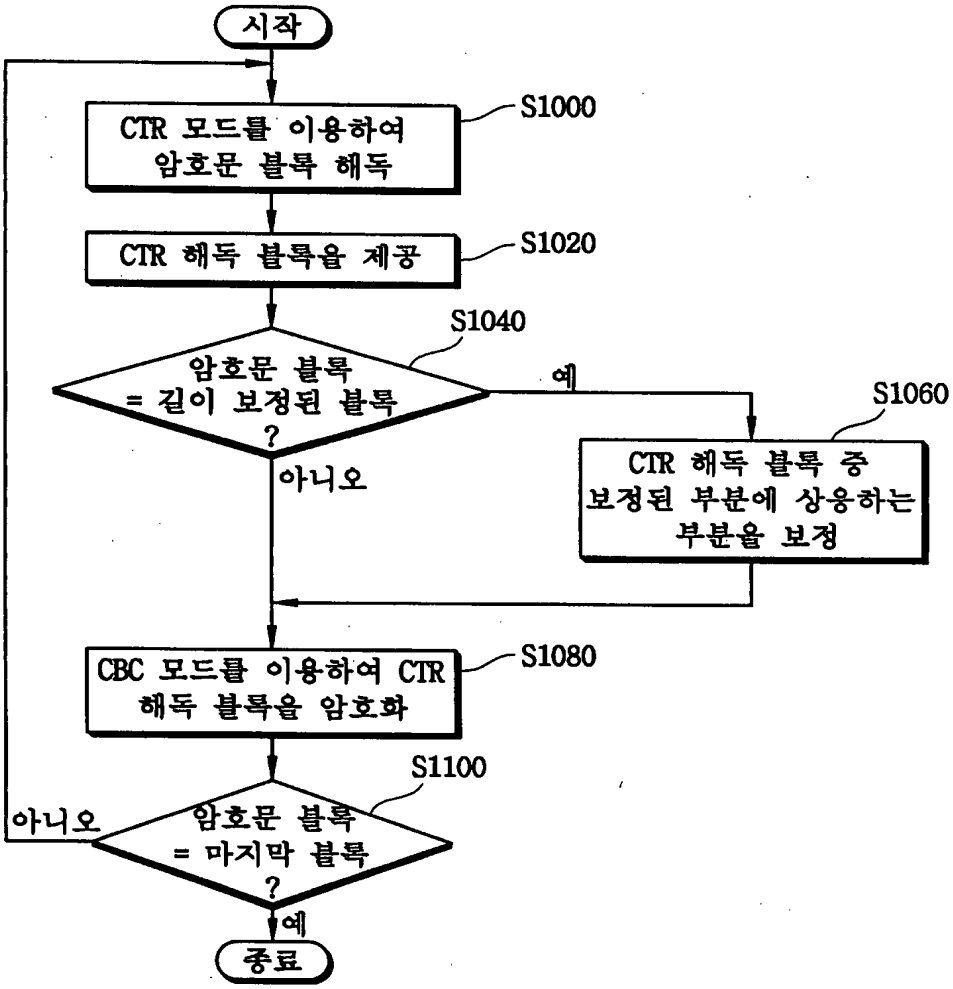
【도 11】


시작
평문 블록 제공
S700
제2 블록을 암호화
S720
평문 블록과 암호화된 제2 블록에 대하여 XOR 연산
S740
평문 블록과 제1 블록에 대하여 XOR 연산
S760
암호화
S780
종료

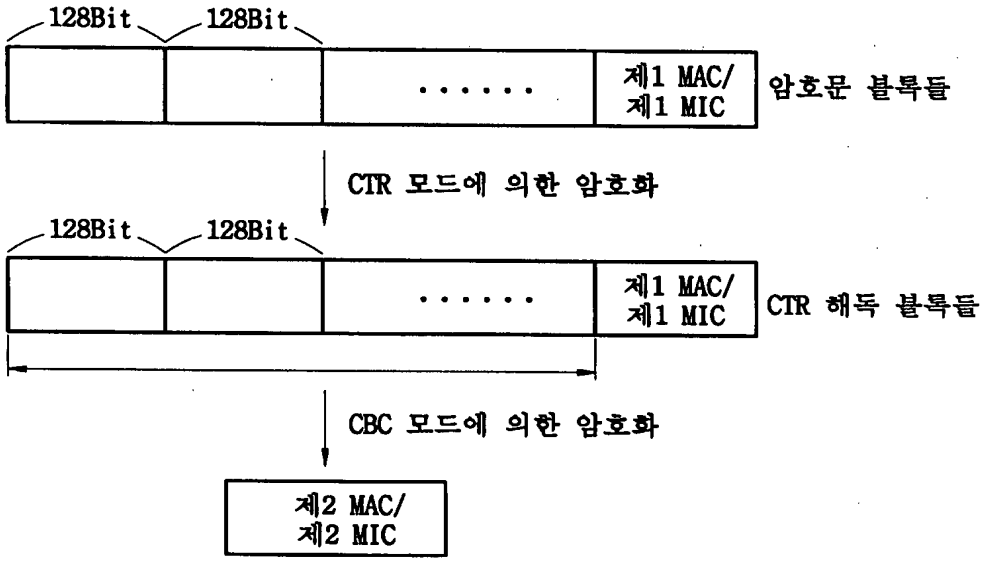
【도 12】


시작
평문 블록 제공
S800
CTR 모드에 의한
평문 블록 암호화
S820
CBC 모드에 의한
평문 블록 암호화
S840
S860
평문 블록
= 마지막 평문 블록
?
아니오
예
마지막 평문 블록에
상응하는 CBC 암호화
블록을 CTR 모드를
이용하여 암호화함
S880
종료

【도 13a】


시작
CTR 모드를 이용하여 암호문 블록 해독
S1000
CTR 해독 블록을 제공
S1020
S1040
암호문 블록 = 길이 보정된 블록 ?
예
아니오
S1060
CTR 해독 블록 중 보정된 부분에 상응하는 부분을 보정
CBC 모드를 이용하여 CTR 해독 블록을 암호화
S1080
S1100
암호문 블록 = 마지막 블록 ?
아니오
예
종료

【도 13b】


128Bit
128Bit
제1 MAC/
제1 MIC
암호문 블록들
CTR 모드에 의한 암호화
128Bit
128Bit
제1 MAC/
제1 MIC
CTR 해독 블록들
CBC 모드에 의한 암호화
제2 MAC/
제2 MIC